The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
9/1/2009
9/8/2009 - UPDATED
10/13/2009 - **UPDATED**

SUBJECT:
Vulnerability in Microsoft IIS Could Lead to Remote Code Execution

ORIGINAL OVERVIEW:
A remote buffer overflow vulnerability has been discovered in Microsoft Internet Information Services (IIS) when using the File Transfer Protocol (FTP) server component. IIS is a set of Internet-based services running on Microsoft Windows servers. Successful exploitation could result in an attacker gaining the same privileges as the FTP service. Depending on the privileges associated, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

It should be noted that there is no patch available for this vulnerability and exploit code is available to the public.

September 8 UPDATED OVERVIEW:
An additional vulnerability has been discovered that is associated with Microsoft's IIS FTP server component. A Denial of Service condition may result if an attacker connects to a FTP server and executes a malicious command. Note that the attacker can connect to the server as either an authenticated or anonymous user.

Please note that we have received reports of this vulnerability being used to compromise systems on the Internet.

October 13 UPDATED OVERVIEW:
Microsoft has released a patch for this vulnerability.

SYSTEMS AFFECTED:

- Microsoft IIS 5.0
  - Microsoft Windows 2000 Advanced Server
  - Microsoft Windows 2000 Advanced Server SP1
  - Microsoft Windows 2000 Advanced Server SP2
  - Microsoft Windows 2000 Datacenter Server SP1
  - Microsoft Windows 2000 Datacenter Server SP2
  - Microsoft Windows 2000 Professional
  - Microsoft Windows 2000 Professional SP1
  - Microsoft Windows 2000 Professional SP2
  - Microsoft Windows 2000 Server
  - Microsoft Windows 2000 Server SP1
  - Microsoft Windows 2000 Server SP2
  - Microsoft IIS 6.0
    - Microsoft Windows Server 2003 Datacenter Edition
    - Microsoft Windows Server 2003 Datacenter Edition Itanium
    - Microsoft Windows Server 2003 Enterprise Edition
    - Microsoft Windows Server 2003 Enterprise Edition Itanium

- Microsoft Windows Server 2003 Standard Edition
- Microsoft Windows Server 2003 Web Edition

September 8 UPDATED SYSTEMS AFFECTED:

- *Microsoft IIS 5.1*
- *Microsoft IIS 7.0*

NOTE: Microsoft IIS 7.0 with FTP Service 7.5 is not affected by this issue.

October 13 UPDATED SYSTEMS AFFECTED:

No additional systems affected

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: N/A

ORIGINAL DESCRIPTION:

A vulnerability has been discovered in Microsoft IIS which could allow an attacker to take complete control of an affected system. This vulnerability is a result of the application failing to perform adequate boundary checks on user-supplied data. More specifically, the vulnerability occurs when handling specially crafted input to the application's FTP server from a malicious user. To exploit this vulnerability, the malicious user must have write privileges to the FTP server; this includes servers that have write access enabled for 'Anonymous' users. At this time, remote code execution is only possible on servers running Microsoft IIS 5.0. Failed exploitation attempts on IIS 5.0 or attacks on IIS 6.0 would result in a Denial of Service (DoS) condition. Successful exploitation could result in an attacker gaining the same privileges as the application. Depending on the privileges associated with the application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

It should be noted that there is no patch available for this vulnerability and exploit code is available to the public.

September 8 UPDATED DESCRIPTION:

An additional vulnerability has been discovered that is associated with Microsoft's IIS FTP server component. A Denial of Service condition may result if an attacker connects to an FTP server and executes a malicious command. The attacker can connect as either an authenticated or anonymous user to the FTP server. A subdirectory must exist in the FTP root for this vulnerability to be exploited. Write access is not required for this vulnerability to be exploited. This vulnerability affects IIS 5.0, IIS 5.1, IIS 6.0 and IIS 7.0

Please note that we have received reports of this vulnerability being used to compromise systems on the Internet.

October 13 UPDATED DESCRIPTION:

Microsoft has released a patch which addresses this vulnerability.

ORIGINAL RECOMMENDATIONS:
The following actions should be taken:

- Install the appropriate vendor patch as soon as it becomes available after appropriate testing.
- Unless there is a business need to do otherwise, consider removing write access to FTP server user accounts.

September 8 UPDATED RECOMMENDATIONS:

- Modify NTFS file permissions to disallow directory creation by FTP users.
- Unless there is a business need to do otherwise, consider removing ftp access to anonymous users.

October 13 UPDATED RECOMMENDATIONS:

- ***Apply the appropriate patch provided by Microsoft to vulnerable systems immediately after appropriate testing.***

ORIGINAL REFERENCES:

Security Focus:
http://www.securityfocus.com/bid/36189

Secunia:
http://secunia.com/advisories/36443

US-CERT:
http://www.kb.cert.org/vuls/id/276653

September 8 UPDATED REFERENCES:

Microsoft:
http://www.microsoft.com/technet/security/advisory/975191.mspx

Security Focus:
http://www.securityfocus.com/bid/36273

Secunia:
http://www.secunia.com/advisories/36594

October 13 UPDATED REFERENCES:
Microsoft:
http://www.microsoft.com/technet/security/bulletin/MS09-053.mspx

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2521
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3023